2021

Lessons Learned From Applying the NIST Privacy Framework

Carter, Thomas; Kroll, Joshua A.; Michael, James Bret

IEEE

Carter, Thomas, Joshua A. Kroll, and James Bret Michael. "Lessons Learned From Applying the NIST Privacy Framework." IT Professional 23.4 (2021): 9-13.
http://hdl.handle.net/10945/68014

Lessons Learned From Applying the NIST Privacy Framework

Thomas Carter, Joshua A. Kroll, and James Bret Michael, *Naval Postgraduate School, Monterey, CA, 93943, USA*

Contact tracing can be beneficial, such as helping to curb the spread of disease, but the handling of the resulting data poses privacy-related risks. This article provides some lessons learned and recommendations regarding the application of the NIST Privacy Framework.

Pandemics affect the security of sovereign states by weakening their economies, defenses, and the overall wellbeing of their citizenries. For example, in March 2020, many of the crew members of the aircraft carrier USS *Theodore Roosevelt* either contracted or were exposed to the COVID-19 virus.[1] In addition to the impact on the health and safety of the sailors, the carrier battle group could not conduct operations for several months in the Indo-Pacific theater of operations. A year later, as part of his Interim National Security Strategic Guidance, U.S. President Joe Biden cited the COVID-19 pandemic as one of the "biggest threats" America has faced.[2]

The COVID-19 pandemic led some healthcare experts and government officials to advocate for instituting automated contact tracing and notification.[3] Automated contact tracing is the tracking of whether an individual has been in proximity to a person that has tested positive for an infectious disease for long enough to constitute exposure. Contact notification is the act of informing an exposed individual soon after authorities establish that the individual's contact tested positive for the disease.

Automated contact tracing and notification, when used in combination with preventative measures (such as vaccinating people and encouraging social distancing) and reactive measures (such as quarantining and providing medical care), can contribute to curbing the spread of infectious diseases.[4] However, for some people automating contact tracing conjures up images of an Orwellian society in which the surveillance of the population by a government strips individuals of much or all of their privacy and other civil liberties. The public policy decision-making process must balance social norms and civil liberties with the value and legality of options available to curtail the effects of an epidemic or a pandemic on national security. Recent research, such that of Cohen, Gostin, and Weitzner, explores the tensions between civil liberties and contact tracing, informing the ongoing public-policy debate over contact tracing.[5]

Our aim in this article is to enhance information technology (IT) professionals' awareness of some of the challenges they will face and available tools for managing privacy-related risks. Many IT professionals will be or already are tasked with acquiring automated contact-tracing systems, integrating those systems with other information systems, and sustaining the contact-tracing systems. As with cybersecurity, real-world information systems are less than perfect at protecting private data, but measures can be taken to minimize the severity and frequency of privacy-related harms. At the time of this writing, the U.S. Department of the Navy (DoN) is acquiring an automated contact-tracing capability.[6] Here we share our lessons learned from applying the U.S. National Institute of Standards and Technology (NIST) Privacy Framework[7] to perform a privacy-risk assessment for an abstracted model of the DoN's contact-tracing system.

Shift From Manual to Automated Contact Tracing

The DoN is no stranger to pandemics. Readiness of the Fleet suffered during the 1918 Pandemic, when approximately 40% of U.S. Navy personnel contracted influenza.[8] The spread of influenza throughout Europe and beyond was exacerbated by the movement of armed combatants and civilians.

Digital Object Identifier 10.1109/MITP.2021.3086916
Date of current version 19 August 2021.

Manual methods of contact tracing do not scale well for epidemics and pandemics, as the world population is currently about 7.9 billion. Even the combined total of Navy active-duty personnel and reservists is close to half a million. Manual methods do not support timely strategic or tactical decision-making. For the current acquisition, the DoN requires the collection, storage, processing, and transmission of data to be automated.

For the DoN automated contact-tracing system, data will be collected through edge computing devices, specifically wearables, that have built-in sensing and communication capability.

Automation addresses the scaling problem, the data-collection requirement, and the need for presenting data in a timely manner to decision-makers. However, automation introduces risks for the DoN, and there are legal, policy, and technical constraints on the degree of automation and the application of contract tracing. We now turn to privacy-related risks and their management.

Privacy Risks

Let us start our exploration of privacy risks by taking a bird's eye view of how the contact-tracing system will operate. Per the request for information, the system will rely on proximity data consisting of contact and time metadata generated by Bluetooth beacons on a person's wearable device. Edge servers collect the data from the network of wearables, process the data, then securely transmit the data to remote data centers. Data analytics can then be used to determine, given reports of new instances of positive test cases for COVID-19 or other infectious diseases, which of the people participating in the DoN's contact-tracing program were in close proximity to confirmed infectious individuals, followed by notificaiton.

The Navy's Jupiter enterprise data management system serves as a central clearinghouse of information. Jupiter can support secondary processing of proximity and COVID-19 incident data to create fleet readiness products for high-level decision makers.[9] In our model of the system, we assume that proximity data will be correlated with COVID-19 incident data from the Bureau of Medicine and Surgery (BUMED)—the DoN's healthcare activity—and other ancillary data needed for disease prevention and mitigation actions.

The proximity-tracing technology will use some form of unique identifier that the user device broadcasts. Other users within range of that device record that unique identifier and record the times that they were within a certain distance from that user, with distance measures computed using the radio-frequency equipped wearable's Received Signal Strength Indicator (RSSI) and with Time-of-Flight (TOF) values (i.e., based on ranging, computing distance between two wireless nodes using detected signal strength and measured roundtrip time of data-packet exchange, respectively). If a user tests positive for COVID-19, the system uses the proximity data to determine which other users may be at risk of infection, then notifies the affected users.

Two prominent factors that play in the DoN's contact-tracing privacy-risk calculus are the potential mishandling and inadvertent release of privacy-sensitive data. There is a risk that contact-tracing data could be used for unauthorized purposes. Some contact tracing systems allow a central authority to have access to all of the data that is collected from users. This central authority may have the ability to reidentify and isolate specific users' proximity data. This opens up the opportunity for someone to abuse the system and track certain users, potentially placing those users in dangerous or compromising situations.

There is also the risk that someone not authorized and without a need for access could discover privacy-sensitive data by making inferences from the data that has not been sufficiently deidentified, and even go a step further by using the data for nonsanctioned purposes such as creating graphs of social networks of users. Recent studies have shown that proximity beacons can be used to infer the social graph and movement of users using machine learning techniques.[10] However, this is not just a privacy risk. It is also an operational security for the DoN.

Managing Privacy Risks

While the preceding examples of privacy risk can be fairly common across contact-tracing systems, the level of risk, measured as a function of severity and frequency of occurrence, will vary from one system to another. Fortunately, risk can be managed, but this requires an organization to: identify the risks; specify each risk in terms of frequency and severity (i.e., how often might a particular privacy harm occur and what is the degree of harm involved); prioritize the handling of the each instance of risk; and adjust as necessary and employ its plan for managing the risks. This will support executive-level leaders and members of their workforce to make informed privacy-risk decisions and implement privacy controls commensurate with decision-makers' desired level of risk acceptance.

Risk management is necessary for preserving human dignity and protecting civil liberties. This is

codified in numerous privacy-related laws, regulations, and policy for handling privacy-sensitive data. For example, the Secretary of the Navy Instruction (SECNAVINST) 5211.5F[11] implements the DoN Privacy Program. SECNAVINST 5211.5F contains broad guidance on privacy protection and states the privacy of individuals as being a "personal and fundamental right that will be respected and protected." While the instruction focuses on individuals, we assert that organizational privacy is equally as important to an organization like the DoN because critical information pertaining to operations can also be gleaned from data leaked during breaches in employee privacy.

In January 2020, NIST released the NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0.[7] The framework's purpose is to facilitate and encourage the consideration of risks to privacy in the acquisition, use, and sustainment of information systems that handle privacy-sensitive data.

The privacy framework closely follows the structure of NIST's cybersecurity framework, first released in 2014.[12] The privacy framework consists of functions that represent different areas of privacy-risk management. The purpose of the functional areas is to help organizations identify privacy risk and build profiles of their organizations' privacy activities and risk tolerance, including where they hope to be in the future. The framework then uses Implementation Tiers to provide a grading scale for organizations to determine if they are in a position to adequately handle their current privacy risk. NIST also provides a mapping of privacy-related risks to controls in Special Publication 800-53 rev5. NIST plans to incorporate more mappings of this type into the framework.[13,14]

Lessons Learned From Applying the Framework

The newness of the NIST Privacy Framework means there is a dearth of reports, experiences, and lessons learned from applying it. We started from a clean slate, lacking relevant reports to direct our application of the framework to a conceptual model we have of the DoN's Bluetooth-based proximity-tracing system. Our model captures key characteristics of a system the DoN planned to acquire while leaving irrelevant details abstracted away.[6]

To establish a baseline, we first conducted privacy-risk modeling without the aid of the privacy framework. Then, we applied the NIST Privacy Framework, with the aim of answering the question: How does the guidance contained in the privacy framework help us in identifying the same threats that we already identified in our risk model. We used the NIST SP 800-53, Rev5 Crosswalk to choose core functions, categories, subcategories, and their corresponding controls that we felt applied to our conceptual model of the DoN contact-tracing system. We produced what the framework terms a Profile; a Profile is an assessment of the privacy risks of the system being assessed.

We observed that the framework led us through a nonthreatening checklist-style process, but left us with the impression that we were not making significant progress in identifying or mitigating privacy risks. For example, there is a Core Function in the framework that focuses on Risk Management. Many of the NIST SP 800-53 mapped controls directed us to the Risk Management chapter in the NIST SP 800-53. One lesson learned was that a framework that lists risk-management aspects and then points to a chapter in a publication that also explains broad risk-management controls did not make us noticeably more effective at performing risk management. We understand that NIST made a conscious decision to minimize the inclusion of detailed guidance and instead provided the user of the framework with plenty of room for maneuver in interpreting the "what" and "how" of conducting privacy-risk management. This, we conclude, is a double-edged sword—lack of detail enables flexibility but limits the utility of the framework as a source of meaningful guidance.

The framework includes many security-specific categories, subcategories, and controls. While security is important and inseparable from privacy, most of the content appeared to be a copy/paste from the cybersecurity framework.

We also noticed that the framework did not give disassociability the attention that it deserves. While disassociability is represented as a subcategory, we expected the framework to provide more guidance regarding deidentifying data due to the prominence of privacy concerns related to data analytics and Big Data. Deidentifying data is a critical capability for the DoN's contact-tracing system and its secondary use cases. Note that deidentifying data is a concern that is also detached from the commonplace security controls that accompany privacy.

In addition, we found that the framework helped us the most as a risk-identification guide. It did not help us much with considering the likelihood of privacy harms occurring or the severity of their consequences, or how to find or specify risk tolerance. We found that the user of the framework needs to fill in a lot of gaps in the guidance on privacy-risk management.

We also found that much of the NIST Privacy Framework is similar to the NIST Cybersecurity

Framework. Privacy and security are related concepts and many of the control families between the two overlap. This is to be expected, as security breaches can often have substantial privacy implications, as when the U.S. Office of Personnel Management's databases of human resources records were compromised in a breach announced in June 2015.[15] We propose that the two frameworks be combined, since they are insufficiently differentiated. This enables consolidation of the controls for security and privacy, matching the structure of NIST SP 800-53 rev5. Nevertheless, we recommend that the combined framework highlight and provide guidance for managing privacy-specific risks above and beyond cybersecurity risks.

Furthermore, we conclude that combining the two frameworks would also streamline the assessment process for IT professionals. From day one of our work with the privacy framework, we asked the question: Given that the NIST SP 800-53 rev5 contains both privacy and security controls, what purpose is served by publishing two separate frameworks—one for privacy, the other for security? At present the U.S. government requires its acquisition professionals to integrate risk assesssments under the cybersecurity framework into their acquisition-and-sustainment decision-making (part of guidance included in the U.S. government's Risk Management Framework publications[16] driven by the Federal Information Security Management Act, FISMA[17]). At present, this is often operationalized for service-oriented tools—like the automated contact-tracing system we consider—by the vendor undergoing certification under the General Services Administration's Federal Risk and Authorization Management Program (FedRAMP).[18] For systems acquired by DoD (and other National Security Systems), vendor requirements will soon shift to the new Cybersecurity Maturity Model Certification (CMMC) process.[19] As requirements shift across the landscape, we view it as being only a matter of time before the NIST Privacy Framework and possibly other privacy guidance will be mandated for use in government acquisition of IT. Consolidation with existing frameworks and guidance, as proposed here, could result in dedupication of effort by IT professionals to meet privacy-risk management needs.

There is still much to be learned about managing privacy risk, as our initial foray in applying the NIST Privacy Framework has shown. Information systems that handle privacy-sensitive data extends well beyond just contact-tracing applications. It will be interesting to see how the NIST Privacy Framework and other privacy frameworks evolve based on feedback from the IT community.

DISCLAIMER

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government or other employers. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright annotations thereon.

REFERENCES

1. "Timeline: Theodore roosevelt COVID-19 outbreak investigation," USNI News, Jun. 23, 2020. Accessed: Jan. 05, 2021. [Online]. Available: https://news.usni.org/2020/06/23/timeline-theodore-roosevelt-covid-19-outbreak-investigation
2. The White House, "Interim national security strategic guidance," The White House, Mar. 2021. Accessed: May 12, 2021. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2021/03/NSC-1v2.pdf
3. P. M. Figliola, "Digital contact tracing technology: Overview and considerations for implementation," *Digit. Contact Tracing Technol., Overview Considerations for Implementation*, vol. 1, pp. 1–3, May 2020. Accessed: Aug. 1, 2020. [Online]. Available: https://heinonline.org/HOL/P?h=hein.crs/govdatx0001&i=1
4. L. Ferretti *et al.*, "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science*, vol. 368, no. 6491, pp. 1–7, 2020. doi: 10.1126/science.abb6936.
5. I. G. Cohen, L. O. Gostin, and D. J. Weitzner, "Digital smartphone tracking for COVID-19: Public health and civil liberties in tension," *JAMA*, vol. 323, no. 23, pp. 2371–2372, 2020, doi: 10.1001/jama.2020.8570.
6. "COVID-19: Proximity tracking program," Jul. 08, 2020. Accessed: Oct. 14, 2020. [Online]. Available: https://beta.sam.gov/opp/806be5faa3bb4d51b6b9a25dcb16f9ab/view
7. NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0, National Institute of Standards and Technology, Gaithersburg, Md., NIST CSWP 01162020, Jan. 16, 2020. doi: 10.6028/NIST.CSWP.01162020.
8. "Spanish flu," History.com, May 19, 2021. Accessed: May 22, 2021. [Online]. Available: https://www.history.com/topics/world-war-i/1918-flu-pandemic
9. Department of the Navy Chief Information Officer, "Jupiter: Bringing the power of data analytics to the DON," *CHIPS*, Sep. 2020. Accessed Jan. 5, 2021. [Online]. Available: https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=13804

10. N. Eagle and A. Pentland, "Reality mining: Sensing complex social systems," *Pers. Ubiquit Comput.*, vol. 10, no. 4, pp. 255–268, May 2006. Accessed: Oct. 11, 2020. [Online]. Available: http://link.springer.com/10.1007/s00779-005-0046-3, doi: 10.1007/s00779-005-0046-3
11. Department of the Navy Privacy Program, Secretary of the Navy Instruction 5211.5F, May 2019. Accessed: Jan. 7, 2021. [Online]. Available: https://www.doncio.navy.mil/ContentView.aspx?id=799
12. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology, Gaithersburg, Md, NIST CSWP 04162018, Apr. 2018. Accessed: Nov. 13, 2020. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
13. Joint Task Force Interagency Working Group, "Security and privacy controls for information systems and organizations," National Institute of Standards and Technology, Sep. 2020. Accessed: Dec. 21, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
14. "NIST privacy framework and cybersecurity framework to NIST special publication 800-53, revision 5 crosswalk," *NIST.gov*, Dec. 10, 2020. Accessed: May 12, 2021. [Online]. Available: https://www.nist.gov/privacy-framework/nist-privacy-framework-and-cybersecurity-framework-nist-special-publication-800-53
15. Office of Personnel Management, "Cybersecurity incidents," U.S. Office of Personnel Management. Accessed Nov. 8, 2020 [Online]. Available: https://www.opm.gov/cybersecurity/cybersecurity-incidents/
16. "Joint task force transformation initiative, risk management framework for information systems and organizations: A system life cycle approach for security and privacy, national institute of standards and technology," Gaithersburg, Md., NIST SP 800-37r2, Dec. 2018. Accessed Aug. 1, 2020 [Online] Available: https://www.opm.gov/cybersecurity/cybersecurity-incidents/. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
17. 113th Congress, *Federal Information Security Modernization Act of 2014*. 2014, p. 16. Accessed: May 23, 2021. [Online]. Available: https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
18. How to Become FedRAMP Authorized, "Federal risk and authorization management program program management office," WA, DC, USA, Accessed: May 23, 2021. [Online]. Available: https://www.fedramp.gov/
19. Office of the Under Secretary of Defense for Acquisition & Sustainment, "Cybersecurity maturity model certification (CMMC)," Carnegie Mellon Univ. and The Johns Hopkins Univ. Applied Physics Laboratory, Mar. 2020, Accessed: May 23, 2021. [Online]. Available: https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

THOMAS CARTER is a Lieutenant in the U.S. Navy and a graduate student with the Naval Postgraduate School's Department of Computer Science, Monterey, CA, USA. Contact him at thomas.carter@nps.edu.

JOSHUA A. KROLL is an Assistant Professor of Computer Science with the Naval Postgraduate School, Monterey, CA, USA. Contact him at jkroll@nps.edu.

JAMES BRET MICHAEL is a Professor of Computer Science and Electrical and Computer Engineering, Naval Postgraduate School, Monterey, CA, USA. Contact him at bmichael@nps.edu.